UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,026	08/10/2001	Lauri Piikivi	617-010487-US(PAR)	5196

2512 7590 11/26/2008

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/928,026	PIIKIVI, LAURI	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date. _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 4, 2007 has been entered.

Claims 1-9, 11, and 14-16 have been amended.

Claims 1-16 are pending and herein considered.

Examiner's Note

The Examiner would like to take this opportunity to remind Applicant of his duty to ensure that his remarks are in fact commensurate with his claims listings. Although the Examiner has chosen to treat Applicant's most recent response as *bona fide*, future correspondence will be considered non-compliant where Applicant's remarks fail to reflect the most recent version of the claims.

Response to Arguments

Applicant's arguments filed January 4, 2007 have been fully considered but they are not persuasive.

In response to the Applicant's arguments concerning Dominguez's alleged failure to disclose "receiving a control message signal that includes a plurality of selective security protocols" and "selecting one of the protocols received in the signal to protect information" as recited in claim 1, the Examiner respectfully disagrees. Applicant argues that Dominguez's "distributed authentication capabilities" fail to teach his "plurality of selectable security protocols" because the authentication options are "specific information for authenticating a user" while Applicant's security protocol "is used to protect information across a communication link." The Examiner is not persuaded by such an argument. If it is Applicant's intention to use the phrase "security protocol" without specifically identifying the types of security he wishes to encompass, it is to be understood that such a phrase might read upon alternate security protocols not intended by Applicant. A security protocol is any abstract or concrete protocol that performs a security-related function. Those functions include but are not limited to authentication, verification, key generation, secure communication, and more. If it is Applicant's intention to claim a secure communication protocol used to protect information transmitted across a communication link, that the Examiner requires Applicant to claim it as such. The Examiner maintains her rejection of Applicant's "selectable security protocols" as taught by Dominguez' "distributed authentication options." With regards to Applicant's arguments concerning Dominguez' alleged failure to teach "selecting one of the protocols received in the signal to protect information" the Examiner is equally unpersuaded. First, the Examiner would like to point out that the

language of Applicant's claims calls for a selector and not "selection means" as Applicant's remarks suggest. Furthermore, the Examiner would like to note that Applicant's claims fail in their entirety to recite "selecting one of the protocols received in the signal to protect information." I actuality, Applicant's claims call for a selector connected to receive a control message signal... said signal including a plurality of selectable security protocols and in response thereto to select one of the plurality of security protocols so that information transferred subsequently between the device and second party is protected using the selected security protocol." The Examiner has equated and will remain to equate such steps with Dominguez' returning of distributed authentication options in the QueryCardholderRes message so that further communication will include the performance of authenticated steps (par 76). These steps, although seemingly not what Applicant intended for in his claims, amount to the selection of a particular security protocol, in this scenario an authentication protocol in order to provide for the protection of information transmitted subsequently. There is no doubt in the Examiner's mind that Dominguez at the time of his invention, understood the range of security protocols in use and it is for that reason that he intentionally built in the necessary selectors and the like to provide for a robust system able to facilitate communication between devices that may or may not use the same standards and who may be programmed to understand a variety of standards.

In response to the Applicant's arguments concerning Williams' alleged failure to disclose "receiving a control message signal that includes a plurality of selectable security protocols, and selecting one of the protocols to protect information" as claimed

in independent claims 1 and 14, the Examiner respectfully disagrees. Applicant argues that Williams fails to teach the sending of a control message indicating the plurality of selectable security protocols but fails entirely to make mention of column 12, lines 49-55 wherein Williams discloses the delivery of the applet and associated information to the consumer's desktop just as he fails to mention claim 14 wherein Williams discusses the SET protocols as well as an implementation of the CyberCash micro-payment protocol, two specific security protocols supported by William's system. There exists no doubt in the Examiner's mind that Williams at the time of his invention knew of the variety of security protocols available (see col.14 line 64 through col.15 line 21 for an additional list of security protocols supported), and the importance of creating a system that would allow one to chose a particular protocol, and it is for these reasons that he created his system to do just that.

In view of the arguments previous, Examiner respectfully disagrees with the Applicant's argument that Dominguez fails to disclose claims 1-16 in their entirety, and maintains the previously presented 35 U.S.C. 102(e) rejections repeated below. The Examiner also respectfully disagrees with the Applicant's argument that Williams fails to disclose claims 1-2, 5, 8-10, 11 and 13 in their entirety, and maintains the previously presented 35 U.S.C. 102(e) rejections repeated below.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2-4, 6-7, 9, and 14-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicant's use of the terms "SET," "EMV," "Europay," "MasterCard," and "VISA" renders his claims indefinite insofar as the use of a trademark or trade name within a claim to identify a particular material product fails to comply with the requirements of 35 USC 112. The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. In fact, the value of a trademark would be lost to the extent that it became descriptive of a product, rather than used as an identification of a source or origin of a product. Thus, the use of a trademark or trade name in a claim to identify or describe a material or product would not only render a claim indefinite, but would also constitute an improper use of the trademark or trade name.

Furthermore, Applicant's use of the term "EMV" is improper insofar as Applicant has failed to point out which particular version of the EMV protocol he intends to include within his invention, seeing at there are at least five different versions.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-16 remain rejected under 35 U.S.C. 102(e) as being anticipated by Dominguez et al. (US Patent Application Publication 2002/0194138).

As per **Claim 1**, Dominguez teaches a device comprising a connecting mechanism for establishing a communication link with a second party and a selector connected to receive a control message signal from said second party said signal including a plurality of selectable security protocols and in response thereto to select one of the plurality of security protocols so that information transferred subsequently between the device and second party is protected using the selected security protocol (pars 69-70, 76, 82).

As per **Claim 2**, Dominguez teaches selection means further comprises an analyzer for analyzing the data contained in said control message signal and in response thereto for selecting the security protocol (pars 76, 82).

As per **Claim 3**, Dominguez teaches a calculator for generating a Europay MasterCard VISA (EMV) cryptogram from data held in at least one data field of the control message signal (pars 68-69, 219).

As per **Claim 4**, Dominguez teaches a cryptogram transmitter provided to transmit the EMV cryptogram from the mobile station to initiate secure transfer of information from the device (pars 68-69, 219).

As per **Claim 5**, Dominguez teaches an application to provide a start payment signal from the device to the second party which thereby initiates the control message signal from the second party (par 33).

As per **Claim 6**, Dominguez teaches a mechanism for communicating, when said selected security protocol is the Secure Electronic Transaction (SET) standard, with a modified SET wallet server which is adapted to receive a Europay MasterCard VISA (EMV) cryptogram generated by the device and thereafter to communicate with a SET payment gateway via the second party according to the SET standard (par 45). Note: The Examiner has relied on the above-cited paragraph to demonstrate Dominguez's use of secure wallets within his invention and the modes of communication associated with them. Although Dominguez fails to specifically mention the term "SET" within his disclosure, it should be brought to the Applicant's attention that the technical specification for security financial transactions on the internet, today known as SET, was introduced by VISA in conjunction with MasterCard in 1996, over 4 years before the filing of the prior art at hand.

As per **Claim 7**, Dominguez teaches means for communicating, when said selected security protocol is the Europay MasterCard VISA (EMV) standard, with the second party directly via an EMV cryptogram generated via the device (par 68-69, 219).

As per **Claim 8**, Dominguez teaches 1 wherein the control message signal includes a series of data fields each containing data indicating a predetermined parameter for the information transfer (pars 72-76).

As per **Claim 9**, Dominguez teaches wherein the control signal includes a data field which indicates whether the device can communicate directly with the second party or with the second party via a modified Secure Electronic Transaction (SET) wallet (par 45).

As per **Claim 10**, Dominguez teaches internet browsing circuitry which enables a user of the device to access and browse the internet via the device (pars 14, 33, 35, 36, 38).

As per **Claim 11**, Dominguez teaches connecting mechanism enables a connection to be established between said device and a second party via the Internet (pars 14, 33, 35, 36, 38).

As per **Claim 12**, Dominguez teaches wherein said device comprises a mobile station (par 38).

As per **Claim 13**, Dominguez teaches wherein said second party comprises a merchant server associated with a merchant offering an item to be purchased (par 3).

As per **Claim 14**, Dominguez teaches a device comprising a connecting mechanism for establishing a communication link with a second party, a selector for selecting one of a plurality of security protocols and being connected to communicate said selection to said second party (pars 69-70, 76, 82), a calculator for generating a Europay MasterCard VISA (EMV) cryptogram for transmittal from said device (par 68-69, 219), so that information transferred subsequently between the device and second party is protected using the selected security protocol (pars 69-70, 76, 82).

As per **Claim 15**, Dominguez teaches a device comprising a connecting mechanism for establishing a communication link with a second party, a selector for selecting a Secure Electronic Transaction (SET) security protocol and being connected to communicate said selection to said second party, and a calculator for generating a Europay MasterCard VISA (EMV) cryptogram for transmittal from said devices so that information transferred subsequently between the device and second party is protected using the SET security protocol (pars 45, 69-70, 76, 82). Note: The Examiner has relied on the above-cited paragraphs to demonstrate Dominguez's use of secure wallets within his invention and the modes of communication associated with them. Although Dominguez fails to specifically mention the term "SET" within his disclosure, it should be brought to the Applicant's attention that the technical specification for security financial transactions on the internet, today known as SET, was introduced by VISA in conjunction with MasterCard in 1996, over 4 years before the filing of the prior art at hand.

As per **Claim 16**, Dominguez teaches a device comprising a connecting mechanism for establishing a communication link with a second part, a selector for selecting a Europay MasterCard VISA (EMV) security protocol and being connected to communicate said selection to said second party (pars 69-70, 76, 82), so that information transferred subsequently between the device and second party is protected using the EMV security protocol (pars 68-69, 219).

Claims 1-2, 5, 8-10, 11, and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by Williams et al. (US Patent No. 5,963,924).

As per **Claim 1**, Williams teaches a device comprising connecting mechanism for establishing a communication link with a second party and a selector connected to receive a control message signal from said second party said signal including a plurality of selectable security protocols and in response thereto to select one of the plurality of security protocols, so that information transferred subsequently between the device and second party is protected using the selected security protocol (col.14 lines 8-24; col.14 line 64 thru col.15 line21; col.16 lines 53-56; col.21 line 35 thru col.22 line 8).

As per **Claim 2**, Williams teaches an analyzer for analyzing the data contained in said control message signal and in response thereto for selecting the security protocol (col.13 lines 51-54; col.15 lines 54-56; col.16 lines 53-56).

As per **Claim 5**, Williams teaches an application to provide a start payment signal from the device to the second party which thereby initiates the control message signal from the second party (col.15 lines 53-55).

As per **Claim 8**, Williams teaches wherein the control message signal includes a series of data fields each containing data indicating a predetermined parameter for the information transfer (col.15 lines 53-55).

As per **Claim 9**, Williams teaches wherein the control signal includes a data field which indicates whether the device can communicate directly with the second party or

with the second party via a modified Secure Electronic Transaction (SET) wallet (col.14 lines 8-24).

As per **Claim 10**, Williams teaches internet browsing circuitry which enables a user of the device to access and browse the internet via the device (abstract, col.10 line 38 thru col.11 line 12; col.9 lines 27-67).

As per **Claim 11**, Williams teaches wherein said connecting mechanism enables a connection to be established between said device and a second party via the Internet (abstract, col.10 line 38 thru col.11 line 12; col.9 lines 27-67).

As per **Claim 13**, Williams teaches wherein said second party comprises a merchant server associated with a merchant offering an item to be purchased (abstract, col.10 line 38 thru col.11 line 12).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437